UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,613	01/17/2001	James Russell Godwin	5577-218	7860

20792	7590	07/02/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER
COULTER, KENNETH R

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 07/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/764,613	GODWIN ET AL.
	Examiner	Art Unit	
	Kenneth R Coulter	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-23* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-23* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>9/17/01; 9/20/01</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

Claim Objections

1.   The numbering of claims is not in accordance with 37 CFR 1.126 which requires

the original numbering of the claims to be preserved throughout the prosecution. When

claims are canceled, the remaining claims must not be renumbered. When new claims

are presented, they must be numbered consecutively beginning with the number next

following the highest numbered claims previously presented (whether entered or not).

Misnumbered claims 22, 23, and 24 have been renumbered 21, 22, and 23,

respectively.

Double Patenting

2.   The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11
F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225
USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA
1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*,
418 F.2d 528, 163 USPQ 644 (CCPA 1969).
        A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be
used to overcome an actual or provisional rejection based on a nonstatutory double
patenting ground provided the conflicting application or patent is shown to be commonly
owned with this application. See 37 CFR 1.130(b).
        Effective January 1, 1994, a registered attorney or agent of record may sign a
terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with
37 CFR 3.73(b).

3.   Claims 1 – 23 are provisionally rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claims 1 - 33 of

copending Application No. 09/764,616. Although the conflicting claims are not identical,

they are not patentably distinct from each other because both the present Application

and Application No. 09/764,616 disclose:

1. A method of providing Internet Protocol Security (IPSec) to a plurality of target hosts

in a cluster of data processing systems which communicate with a network through a

routing communication protocol stack utilizing a dynamically routable Virtual Internet

Protocol Address (DVIPA), the method comprising: negotiating security associations

(SAs) associated with the DVIPA utilizing an Internet Key Exchange (IKE) component

associated with the routing communication protocol stack; and distributing information

about the negotiated SAs to the target hosts to allow the target hosts to perform IPSec

processing of communications from the network utilizing the negotiated SAs.

2. A method according to claim 1, wherein the routing communication protocol stack

further carries out the steps of: receiving a communication from the network;

determining if the communication is an IPSec communication to the DVIPA; routing the

received communication to one of the target hosts.

3. A method according to claim 2, wherein the step of determining if the communication

is an IPSec communication comprises the steps of: evaluating a destination address in

the IP header of a received datagram of the communication; and determining if the

destination address is a dynamic VIPA.

4. A method according to claim 3, wherein the step of evaluation a destination address

is preceded by the steps of: determining if the destination address is encrypted; and

decrypting the received communication utilizing an SA associated with the IPSec

communication to decrypt a Transmission Control Protocol (TCP) header of the

datagram.

5. A method according to claim 4, further comprising the step of determining a location of the TCP header in the received communication based on whether the IPSec SA is in transport mode or tunnel mode.

6. A method according to claim 3 wherein the routing communication protocol stack further carries out the step of bypassing inbound filtering if the communication is an IPSec communication to the DVIPA.

7. A method according to claim 3, wherein the routing communication protocol stack further carries out the steps of: inbound filtering the communication if the communication is an IPSec communication; and encapsulating the filtered inbound communication in a generic routing format; and wherein the step of routing comprises routing the encapsulated communication to the one of the target hosts; and wherein a communication protocol stack of the one of the target hosts carries out the steps of: bypassing inbound filtering of the routed encapsulated communication; and decapsulating the routed encapsulated communication.

8. A method according to claim 7, wherein the step of inbound filtering further comprises the steps of: performing a tunnel check on the received communication; and rejecting the received communication so as to not route the received communication to the one of the target hosts based on the results of the tunnel check.

9. A method according to claim 2, wherein the routing communication protocol stack further carries out the steps of: performing a replay sequence number check on the received communication; and rejecting the communication so as to not route the

received communication to the one of the target hosts based on the results of the replay sequence number check.

10. A method according to claim 2, wherein the step of routing comprises the steps of: selecting a target host from the plurality of target hosts based on entries in a distributed connection table associated with the DVIPA; and sending the received communication to the selected target host over a trusted link.

11. A method according to claim 1, wherein the information about the negotiated SAs comprises the SAs and wherein the step of distributing further comprises the step of storing the distributed SAs in a shadow cache of communication protocol stacks of the target hosts.

12. A method according to claim 11, wherein the target hosts further carry out the step of IPSec processing communications to the DVIPA utilizing the SAs in the shadow cache.

13. A method according to claim 12, further comprising the step of providing an inbound lifesize count from the communication protocol stacks of the target hosts to the routing communication protocol stack.

14. A method according to claim 13, wherein the IKE refreshes the SAs associated with the DVIPA based on the inbound lifesize count provided by the communication protocol stacks of the target hosts.

15. A method according to claim 13, wherein the step of providing an inbound lifesize count comprises the step of sending a cross coupling facility (XCF) message identifying the inbound lifesize count to the routing communication protocol stack.

16. A method according to claim 15, wherein the step of sending an XCF message identifying the inbound lifesize count comprises the step of periodically sending a XCF message identifying the inbound lifesize count for a plurality of IPSec processed communications.

17. A method according to claim 16, wherein the plurality of IPSec processed communications comprises a percentage of a total lifesize count associated with an SA.

18. A method according to claim 17, further comprising the step of dynamically establishing the percentage of the total lifesize count based on whether the IKE has previously refreshed the SA prior to expiration of a lifesize count threshold associated with the SA.

19. A system for providing Internet Protocol Security (IPSec) to a plurality of target hosts in a cluster of data processing systems, comprising: a shadow SA cache at each of the target hosts which is configured to store security association (SA) information associated with a dynamically routable Virtual Internet Protocol Address (DVIPA); and a communication protocol stack at each of the target hosts configured to IPSec process datagrams associated with the DVIPA utilizing the SA information in the shadow SA cache.

20. A system according to claim 19, further comprising: a routing communication protocol stack configured to route communications to the plurality of target hosts from a network utilizing the distributed Virtual Internet Protocol Address (DVIPA); an Internet Key Exchange module (IKE) associated with the routing communication protocol stack; and wherein the routing communication protocol stack is further configured to distribute

security association (SA) information for IPSec SAs negotiated by the IKE and

associated with the DVIPA to the communication protocol stacks at each of the target

hosts; and wherein the communication protocol stacks at each of the target hosts are

configured to store the IPSec SA information in the shadow SA cache.

21. A system according to claim 20, wherein the routing communication protocol stack

is further configured to decrypt the Transmission Control Protocol (TCP) header of

received IPSec encapsulated datagrams to determine if the received datagram is

associated with a DVIPA.

22. A system according to claim 20, wherein the routing communication protocol stack

is further configured to store an IPSec sequence number in a coupling facility.

23. A system according to claim 20, wherein the communication protocol stacks at each

of the target hosts are further configured to update a lifesize count of the IKE associated

with IPSec processed datagrams.

4.   This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by
another filed in the United States before the invention by the applicant for patent or (2) a patent
granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 and 2 are rejected under 35 U.S.C. 102(e) as being disclosed by Dixon et al. (U.S. Pat. No. 6,697,857) (Centralized Deployment of IPSec Policy Information).

6.1 Regarding claim 1, Dixon discloses a method of providing Internet Protocol Security (IPSec) to a plurality of target hosts in a cluster of data processing systems which communicate with a network through a routing communication protocol stack utilizing a dynamically routable Virtual Internet Protocol Address (DVIPA), the method comprising:

negotiating security associations (SAs) associated with the DVIPA utilizing an Internet Key Exchange (IKE) component associated with the routing communication protocol stack (col. 6, lines 8 – 11 "IKE 111 is invoked to negotiate an appropriate security association"); and

distributing information about the negotiated SAs to the target hosts to allow the target hosts to perform IPSec processing of communications from the network utilizing the negotiated SAs (Abstract; Fig. 2; col. 5, lines 42 – 67; col. 6, lines 1 - 17).

6.2 Per claim 2, Dixon teaches a method according to claim 1, wherein the routing communication protocol stack further carries out the steps of:
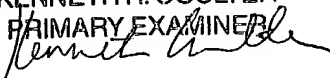
receiving a communication from the network (col. 3, lines 48 - 67);

determining if the communication is an IPSec communication to the DVIPA;

routing the received communication to one of the target hosts (Abstract; Fig. 2; col. 5,

lines 42 – 67; col. 6, lines 1 - 17).

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kenneth R Coulter whose telephone number is 703 305-

8447. The examiner can normally be reached on 5 4 9.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Rupal Dharia can be reached on 703 305-4003. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

KENNETH R. COULTER
PRIMARY EXAMINER

krc